IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: David E. MCDYSAN *et al.*	Confirmation No.: 7586
Application No.: 09/723,481	Group Art Unit: 2153
Filed: November 28, 2000	Examiner: Bates, K.
Customer No.: 25537	
Attorney Docket: RIC00042	

For: PROGRAMMABLE ACCESS DEVICE FOR A DISTRIBUTED NETWORK ACCESS SYSTEM

APPEAL BRIEF

Commissioner for Patents
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal dated April 15, 2005.

I. REAL PARTY IN INTEREST

The real party in interest of the present application, solely for purposes of identifying and avoiding potential conflicts of interest by board members due to working in matters in which the member has a financial interest, is Verizon Communications Inc. and its subsidiary companies, which currently include

Verizon Business Global, LLC (formerly MCI, LLC) and Cellco Partnership (doing business as Verizon Wireless, and which includes as a minority partner affiliates of Vodafone Group Plc). Verizon Communications Inc. or one of its subsidiary companies is an assignee of record of the present application.

II. RELATED APPEALS AND INTERFERENCES

An appeal has been filed in related applications Serial No. 09/723,480 and Serial No. 09/723,501.

III. STATUS OF THE CLAIMS

Claims 1-14, 16-38, and 40-50 are pending in this appeal, in which claims 15 and 39 have earlier been canceled. No claim is allowed. This appeal is therefore taken from the final rejection of claims 1-14, 16-38, and 40-50 on September 13, 2007.

IV. STATUS OF AMENDMENTS

All amendments have been entered and a correct copy of the claims in this appeal is presented in the Appendix below.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The claimed invention addresses problems associated with IP-based communication networks. In particular, the use of a programmable access device, as claimed, overcomes the disadvantages of conventionally concentrating the functions of routing, policy database storage, and policy enforcement in expensive routers.

Independent claim 1 provides for the following:

1. A programmable access device for use in a network access system (See, e.g., Specification, page 5, lines 1-17), said programmable access device comprising:

first and second network interfaces (See, e.g., Specification, page 5, line 9, and page 19, line 16-page 28, line 13) through which packets are communicated with a network (See, e.g., Specification, page 13, lines 17-24);

a packet header filter (See, e.g., Specification, page 13, lines 24-30) and a forwarding table (See, e.g., Specification, page 13, lines 12-13), wherein the forwarding table is utilized to forward packets between the first and second network interfaces (See, e.g., Specification, page 14, line 31-page 15, line 5), and wherein said packet header filter identifies messages received at one of the first and second network interfaces on which policy-based services are to be implemented (See, e.g., Specification, page 14, lines 1-8) and passes identified

messages via a message interface to an external processor included in said network access system for implementation of the policy-based services by the external processor (See, e.g., Specification, page 13, line 11-page 21, line 9), wherein said packet header filter passes all other received messages through the packet header filter to an other processor (See, e.g., Specification, page 13, lines 24-32); and

a control interface through which said packet header filter and said forwarding table are programmed (See, e.g., Specification, page 23, line 13-page 26, line 1, and Tables II and III).

Independent claim 26 provides for the following:

26. A method of packet handling in a programmable access device of a network access system (See, e.g., Specification, page 5, lines 1-17), said method comprising:

in response to receiving a series of packets at a first network interface of a programmable access device (See, e.g., Specification, page 14, lines 1-4), filtering the series of packets by a packet header filter at the programmable access device (See, e.g., Specification, page 13, lines 17-32) to identify messages upon which policy-based services are to be implemented (See, e.g., Specification, page 13, lines 25-27);

passing identified messages to an external processor included in the network access system for implementation of the policy-based services by the external processor (See, e.g., Specification, page 14, lines 1-8, page 13, line 11-page 21, line 9);

for messages that are not identified, routing packets by reference to a forwarding table in the programmable access device and outputting the routed packets at a second network interface of the programmable access device (See, e.g., Specification, page 13, lines 24-32); and

programming the packet header filter and the forwarding table through a control interface of said programmable access device (See, e.g., Specification, page 23, line 13-page 26, line 1, and Tables II and III).

Independent claim 50 provides for the following:

50. A device for use in a network access system comprising:

a first network interface through which packets are communicated with a first network;

a second network interface through which packets are communicated with a second network (See, e.g., Specification, page 5, lines 1-17, page 5, line 9, and page 19, line 16-page 28, line 13, and page 13, lines 17-24);

a message interface coupled to an external processor that is configured to implement policy-based services (See, e.g., Specification, page 13, lines 27-32);

a policer configured to discard packets determined as nonconforming to a first traffic parameter (See, e.g., Specification, page 14, lines 4-7);

a first packet header filter coupled to the first network interface and to the message interface (See, e.g., Specification, page 13, lines 17-18, and 30), wherein the first packet header filter identifies messages, received from the first network interface (See, e.g., Specification, page 13, lines 25-26), on which policy-based services are to be implemented (See, e.g., Specification, page 14, lines 1-4), wherein the first packet header filter passes the identified messages to the external processor via the message interface (See, e.g., Specification, page 13, lines 27-30), and passes all other messages received from the first network interface to the policer (See, e.g., Specification, page 13, line 30);

a marker configured to discard packets determined as nonconforming to a second traffic parameter (See, e.g., Specification, page 14, line 6);

a control interface through which said first packet header filter is programmed (See, e.g., Specification, page 14, line 12); and

a second packet header filter, different from the first packet header filter, coupled to the second network interface, wherein the second packet header filter identifies messages, received from the second network interface (See, e.g.,

Specification, page 13, lines 25-26), on which policy-based services are to be implemented (See, e.g., Specification, page 14, lines 1-4), wherein the second packet header filter passes the identified messages to the external processor via the message interface (See, e.g., Specification, page 13, lines 27-30), and passes all other messages received from the second network interface to the marker (See, e.g., Specification, page 14, lines 1-12).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 2, 4, 7, 16, 22-27, 29, 32, 40, and 46-49 are anticipated under 35 U.S.C § 102(e) by *Albert et al.* (US 6,606,316)?

Whether claims 19-21 and 43-45 are obvious under 35 U.S.C. § 103 based on *Albert et al.* (US 6,606,316)?

Whether claims 11 and 36 are obvious under 35 U.S.C. § 103 based on *Albert et al.* (US 6,606,316) in view of *Natarajan et al.* (US 6,505,244)?

Whether claims 3 and 28 are obvious under 35 U.S.C. § 103 based on *Albert et al.* (US 6,606,316) in view of *Amara et al.* (US 6,674,743)?

Whether claims 5-10, 12-14, 17, 18, 30, 31, 33-35, 37, 38, 41, and 42 are obvious under 35 U.S.C. § 103 based on *Albert et al.* (US 6,606,316) in view of *Gai et al.* (US 6,167,445)?

Whether claim 50 is obvious under 35 U.S.C. § 103 based on *Albert et al.* (US 6,606,316) and *Gai et al.* (US 6,167,445) in view of *Amara et al.* (US 6,674,743)?

VII. ARGUMENT

A. CLAIMS 1, 2, 4, 7, 16, 22-27, 29, 32, 40, AND 46-49 ARE NOT ANTICIPATED OVER *ALBERT ET AL.*, BECAUSE *ALBERT ET AL.* FAILS TO DISCLOSE THE CLAIMED FEATURE OF "THE FORWARDING TABLE IS UTILIZED TO FORWARD PACKETS BETWEEN THE FIRST AND SECOND NETWORK INTERFACES."

To anticipate a patent claim, every element and limitation of the claimed invention must be found in a single prior art reference, arranged as in the claim. *Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383, 58 USPQ2d 1286, 1291 (Fed. Cir. 2001); *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 1576, 18 USPQ2d 1001, 1010 (Fed. Cir. 1991).

The Examiner contends that *Albert et al.* discloses, in Fig. 11, and at col. 28, lines 10-65, the steps taken by a forwarding agent upon receiving a packet. The packet is identified for any special services to be performed by using fixed or wildcard affinities. If a dispatch flag is set, the packet is dispatched by the forwarding agent to the forwarding address specified. However, there is nothing in *Albert et al.* indicating the forwarding of packets "**between first and second network interfaces**," as in claim 1, or "routing packets by reference to a

forwarding table in the programmable access device and outputting the routed packets at **a second network interface** of the programmable access device," as in claim 26. While there would be a "network interface" between network 210 and the forwarding agent 231, for example, as shown in Fig. 2A, and there may be "interfaces" between forwarding agent 231 and service manager 241 or 242, and between forwarding agent 231 and servers 220, there is no indication that servers 220 and/or service managers 241 and 242 are in a different "**network**" from forwarding agent 231. Therefore, there is no "**second network interface**" in *Albert et al.*, as required by the present claims and the Examiner's position to the contrary is based on speculation, at best. Speculation is not a proper basis on which to base a finding of anticipation under 35 U.S.C § 102(e).

B. CLAIMS 1, 2, 4, 7, 16, 22-27, 29, 32, 40, AND 46-49 ARE NOT ANTICIPATED OVER *ALBERT ET AL.* BECAUSE *ALBERT ET AL.* FAILS TO DISCLOSE THE CLAIMED FEATURE OF "A CONTROL INTERFACE THROUGH WHICH SAID PACKET HEADER FILTER AND SAID FORWARDING TABLE ARE PROGRAMMED."

The Examiner identifies col. 18, lines 23-41, of *Albert et al.* as teaching the claimed "control interface," contending that "the service manager is connected with the forwarding agents through an interface that can send affinity updates to those forwarding agents. Those affinity updates are programmed to change the

operation of the forwarding agents" (page 2 of the Advisory Action of October 30, 2007).

The cited portion of the reference is concerned with sending messages between the forwarding agents and the service managers and sending wildcard affinities by the service managers. At col. 17, lines 51-54, *Albert et al.* recites that "Actions defined for the affinities specify the service to be performed by the forwarding agent on behalf of the Manager." Thus, the forwarding agent in *Albert et al.* is given some instruction as to what service is to be performed on the part of the service manager; but, there is no indication that the service manager itself actually "programs" the forwarding agent and a packet header filter.

Further, the Examiner's explanation would appear to indicate that the Examiner considers the service manager of *Albert et al.* to be the claimed "control interface," but the Examiner has previously indicated (see the penultimate paragraph on page 2 of the Advisory Action of October 30, 2007) that the service manager of *Albert et al.* is considered to be the claimed "external processor." However, the instant claims, by reciting the "control interface" and the "external processor" as two different elements, make it clear that the control interface and the external processor are separate and distinct entities within the network access system (see, for example, by way of explanation and not limitation, Figs. 2 and 3, where programmable access device (PAD) 40 is separate and distinct from external

processor 42, with elements 40 and 42 both being within the network access system 31, while the control interface 104 is within PAD 40). That is, in accordance with the language of the present claims, the claimed "external processor" is external to the PAD but included, along with the PAD, in the overall network access device. Thus, the service manager (241 or 242) of *Albert et al.* cannot be both the claimed "external processor" and the claimed "control interface." The service manager of *Albert et al.* cannot be, at the same time, both within the PAD and external to it.

Accordingly, for the reasons above, the Examiner has erred in failing to establish a *prima facie* case of anticipation and the rejection of claims 1, 2, 4, 7, 16, 22-27, 29, 32, 40, and 46-49 under 35 U.S.C § 102(e) must be reversed, because *Albert et al.* does not disclose all of the limitations of the claims.

C. CLAIMS 19-21 AND 43-45 ARE NOT RENDERED OBVIOUS BY *ALBERT ET AL.* BECAUSE *ALBERT ET AL.* DOES NOT DISCLOSE OR SUGGEST ALL OF THE CLAIMED FEATURES.

For the reasons above, *Albert et al.* fails to disclose the claimed features of "wherein the forwarding table is utilized to forward packets between the first and **second network** interfaces" and "a **control interface** through which said packet header filter and said forwarding table are programmed" (independent claim 1) or "routing packets by reference to a forwarding table in the programmable access

device and outputting the routed packets at **a second network interface** of the programmable access device" and "programming the packet header filter and the forwarding table through a **control interface** of said programmable access device" (independent claim 26).

Accordingly, the Examiner has erred in failing to present a *prima facie* case of obviousness and the rejection of claims 19-21 and 43-45 under 35 U.S.C. § 103 must be reversed.

D. CLAIMS 3, 5-14, 17, 18, 28, 30, 31, 33-38, 41, AND 42 ARE NOT RENDERED OBVIOUS BY *ALBERT ET AL.* IN COMBINATION WITH ANY ONE OF *NATARAJAN ET AL.*, *AMARA ET AL.*, OR *GAI ET AL.* BECAUSE NONE OF THE SECONDARY REFERENCES PROVIDES FOR THE DEFICIENCIES OF *ALBERT ET AL.*

Since none of the applied references to *Natarajan et al.*, *Amara et al.*, or *Gai et al.* teaches or suggests the claimed features of "wherein the forwarding table is utilized to forward packets between the first and **second network** interfaces" and "a **control interface** through which said packet header filter and said forwarding table are programmed" (independent claim 1) or "routing packets by reference to a forwarding table in the programmable access device and outputting the routed packets at **a second network interface** of the programmable access device" and "programming the packet header filter and the forwarding table

through a **control interface** of said programmable access device" (independent claim 26), features lacking in the primary reference to *Albert et al.* for the reasons above, claims 3, 5-14, 17, 18, 28, 30, 31, 33-38, 41, and 42 have been improperly rejected under 35 U.S.C. § 103.

Accordingly, the Examiner has erred in failing to present a *prima facie* case of obviousness and the rejection of claims 3, 5-14, 17, 18, 28, 30, 31, 33-38, 41, and 42 under 35 U.S.C. § 103 must be reversed.

E. CLAIM 50 IS NOT RENDERED OBVIOUS BY *ALBERT ET AL.* IN COMBINATION WITH *AMARA ET AL.,* AND *GAI ET AL.* BECAUSE NEITHER OF THE SECONDARY REFERENCES PROVIDES FOR THE DEFICIENCIES OF *ALBERT ET AL.*

Since neither of the applied references to *Amara et al.*, or *Gai et al.* teaches or suggests the claimed features of "a **second network interface** through which packets are communicated with a **second network**" and "**a control interface** through which said first packet header filter is programmed; and a second packet header filter, different from the first packet header filter, coupled to the **second network interface**," features lacking in the primary reference to *Albert et al.* for the reasons above, claim 50 has been improperly rejected under 35 U.S.C. § 103.

Accordingly, the Examiner has erred in failing to present a *prima facie* case of obviousness and the rejection of claim 50 under 35 U.S.C. § 103 must be reversed.

VIII. CONCLUSION AND PRAYER FOR RELIEF

For the foregoing reasons, Appellants respectfully request the Honorable Board to reverse each of the Examiner's rejections.

To the extent necessary, a petition for an extension of time under 37 C.F.R. §1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 504213 and please credit any excess fees to such deposit account.

Respectfully Submitted,

DITTHAVONG MORI & STEINER, P.C.

September 29, 2008
Date

/Phouphanomketh Ditthavong/
Phouphanomketh Ditthavong
Attorney for Applicant(s)
Reg. No. 44658

Errol A. Krass
Attorney/Agent for Applicant(s)
Reg. No. 60090

918 Prince Street
Alexandria, VA 22314
Tel. 703-519-9952
Fax. 703-519-9958

IX. CLAIMS APPENDIX

1. A programmable access device for use in a network access system, said programmable access device comprising:

first and second network interfaces through which packets are communicated with a network;

a packet header filter and a forwarding table, wherein the forwarding table is utilized to forward packets between the first and second network interfaces, and wherein said packet header filter identifies messages received at one of the first and second network interfaces on which policy-based services are to be implemented and passes identified messages via a message interface to an external processor included in said network access system for implementation of the policy-based services by the external processor, wherein said packet header filter passes all other received messages through the packet header filter to an other processor; and

a control interface through which said packet header filter and said forwarding table are programmed.

2. The programmable access device of Claim 1, wherein the packet header filter receives packets directly from the first network interface.

3. The programmable access device of Claim 2, wherein the packet header filter is a first packet header filter, and wherein the programmable access device further comprises a second packet header filter that receives packets directly from the second network interface.

4. The programmable access device of Claim 1, wherein the packet header filter filters packets for service processing based upon protocol information pertaining to protocol layers higher than layer 3.

5. The programmable access device of Claim 1, and further comprising a policer that polices packets by reference to traffic parameters.

6. The programmable access device of Claim 5, wherein the policer comprises a marker that marks packets that do not conform with the traffic parameters.

7. The programmable access device of Claim 1, and further comprising at least a usage monitor that monitors at least one traffic type.

8. The programmable access device of Claim 7, wherein the usage monitor has an associated threshold that when exceeded generates a reporting event for the usage monitor.

9. The programmable access device of Claim 8, and further comprising a reporting interface that communicates the reporting event to the external processor.

10. The programmable access device of Claim 9, wherein the associated threshold comprises a session activity level threshold.

11. The programmable access device of Claim 7, and further comprising a fault monitor.

12. The programmable access device of Claim 1, and further comprising one or more output buffers for outgoing packets.

13. The programmable access device of Claim 12, and further comprising a scheduler associated with the one or more output buffers that schedules the transmission of outgoing packets within the one or more output buffers.

14. The programmable access device of Claim 13, wherein the scheduler supports multiple quality of service classes.

15. (Canceled)

16. The programmable access device of Claim 1, and further comprising at least a programmable monitor that monitors at least one programmed traffic type.

17. The programmable access device of Claim 1, and further comprising a policer that polices packets by reference to programmed traffic parameters.

18. The programmable access device of Claim 1, and further comprising one or more output buffers for outgoing packets and an associated scheduler that transmits the outgoing packets from the one or more output buffers through the second network interface according to a programmed methodology.

19. The programmable access device of Claim 1, wherein the identified message is a session initiation protocol (SIP) message.

20. The programmable access device of Claim 1, wherein the identified message is an Internet Group Multicast Protocol (IGMP) message.

21. The programmable access device of Claim 1, wherein the identified message is a Resource Reservation Protocol (RSVP) message.

22. The programmable access device of Claim 1, and further comprising a plurality of protocol-specific state machines for a respective plurality of protocol types.

23. The programmable access device of Claim 22, wherein said plurality of protocol-specific state machines include a transport control protocol (TCP) state machine that, responsive to a control command, provides preferential treatment to a particular TCP session.

24. The programmable access device of Claim 1, and further comprising a reporting interface through which the programmable access device reports state information for active sessions to the external processor.

25. The programmable access device of Claim 24, wherein the reporting interface reports the state information for an active session in response to allocation of service to a new external service controller.

26. A method of packet handling in a programmable access device of a network access system, said method comprising:

in response to receiving a series of packets at a first network interface of a programmable access device, filtering the series of packets by a packet header filter at the programmable access device to identify messages upon which policy-based services are to be implemented;

passing identified messages to an external processor included in the network access system for implementation of the policy-based services by the external processor;

for messages that are not identified, routing packets by reference to a forwarding table in the programmable access device and outputting the routed packets at a second network interface of the programmable access device; and

programming the packet header filter and the forwarding table through a control interface of said programmable access device.

27. The method of Claim 26, and further comprising receiving packets at the packet header filter directly from the first network interface.

28. The method of Claim 27, wherein the packet header filter is a first packet header filter, said method further comprising receiving packets at a second packet header filter of the programmable access device directly from the second network interface.

29. The method of Claim 26, wherein filtering comprises filtering packets for service processing based upon protocol information pertaining to protocol layers higher than layer 3.

30. The method of Claim 26, and further comprising policing packets by reference to traffic parameters utilizing a policer in the programmable access device.

31. The method of Claim 30, wherein policing comprises marking packets that do not conform with the traffic parameters.

32. The method of Claim 26, wherein the programmable access device includes at least a usage monitor, said method further comprising monitoring at least one traffic type in said series of packets.

33. The method of Claim 32, wherein the usage monitor has an associated threshold, said method further comprising generating a reporting event for the usage monitor when the threshold is exceeded.

34. The method of Claim 33, and further comprising communicating the reporting event to an external processor via a reporting interface.

35. The method of Claim 34, wherein generating a reporting event comprises generating a reporting event in response to a session activity level threshold.

36. The method of Claim 32, and further comprising monitoring faults utilizing a fault monitor in said programmable access device.

37. The method of Claim 26, and further comprising buffering outgoing packets in one or more output buffers in said programmable access device.

38. The method of Claim 37, and further comprising scheduling the transmission of outgoing packets within the one or more output buffers to support multiple quality of service classes.

39. (Canceled)

40. The method of Claim 26, wherein the programmable access device further includes at least one programmable monitor, said method further comprising monitoring at least one programmed traffic type utilizing said at least one programmable monitor.

41. The method of Claim 26, wherein said programmable access device includes a policer, said method further comprising policing packets by reference to programmed traffic parameters.

42. The method of Claim 26, wherein the programmable access device includes one or more output buffers for outgoing packets and an associated scheduler, said method comprising transmitting the outgoing packets from the one

or more output buffers through the second network interface according to a programmed methodology.

43. The method of Claim 26, wherein the identified message is a session initiation protocol (SIP) message.

44. The method of Claim 26, wherein the identified message is an Internet Group Multicast Protocol (IGMP) message.

45. The method of Claim 26, wherein the identified message is a Resource Reservation Protocol (RSVP) message.

46. The method of Claim 26, and further comprising maintaining in said programmable access device a plurality of protocol-specific state machines for a respective plurality of protocol types.

47. The method of Claim 46, wherein said plurality of protocol-specific state machines include a transport control protocol (TCP) state machine, and wherein the method further comprises providing preferential treatment to a particular TCP session by said programmable access device in response to a command.

48. The method of Claim 26, and further comprising reporting state information for active sessions to an external processor via a reporting interface of the programmable access device.

49. The method of Claim 48, wherein reporting comprises reporting the state information for an active session in response to allocation of service to a new external service controller.

50. A device for use in a network access system comprising:

a first network interface through which packets are communicated with a first network;

a second network interface through which packets are communicated with a second network;

a message interface coupled to an external processor that is configured to implement policy-based services;

a policer configured to discard packets determined as nonconforming to a first traffic parameter;

a first packet header filter coupled to the first network interface and to the message interface, wherein the first packet header filter identifies messages,

received from the first network interface, on which policy-based services are to be implemented, wherein the first packet header filter passes the identified messages to the external processor via the message interface and passes all other messages received from the first network interface to the policer;

a marker configured to discard packets determined as nonconforming to a second traffic parameter;

a control interface through which said first packet header filter is programmed; and

a second packet header filter, different from the first packet header filter, coupled to the second network interface, wherein the second packet header filter identifies messages, received from the second network interface, on which policy-based services are to be implemented, wherein the second packet header filter passes the identified messages to the external processor via the message interface and passes all other messages received from the second network interface to the marker.

X. EVIDENCE APPENDIX

Appellants are unaware of any evidence that is required to be submitted in the present Evidence Appendix.

XI. RELATED PROCEEDINGS APPENDIX

Appellants are unaware of any related proceedings that are required to be submitted in the present Related Proceedings Appendix.